IN THE SPECIFICATION

Please replace the paragraph beginning on page 1, line 18, with the following replacement paragraph:

One such application is in authentication tokens, such as the RSA ~~SecurID~~SECURID® authentication token commercially available from RSA Security Inc. of Bedford, Massachusetts, U.S.A. The RSA ~~SecurID~~SECURID® authentication token is used to provide two-factor authentication. Authorized users are issued individually-registered tokens that generate single-use token codes, which change based on a time code algorithm. For example, a different token code may be generated every 60 seconds. In a given two-factor authentication session, the user is required to enter a personal identification number (PIN) plus the current token code from his or her authentication token. This information is supplied to an authentication entity. The authentication entity may be a server or other processing device equipped with RSA ACE/~~Server~~SERVER® software, available from RSA Security Inc. The PIN and current token code may be transmitted to the authentication entity via an encryption agent equipped with RSA ACE/~~Agent~~AGENT® software, also available from RSA Security Inc. If the PIN and current token code are determined to be valid, the user is granted access appropriate to his or her authorization level. Thus, the token codes are like temporary passwords that cannot be guessed by an attacker, with other than a negligible probability.

Please replace the paragraph beginning on page 2, line 1, with the following replacement paragraph:

A given RSA ~~SecurID~~SECURID® token typically contains one or more seeds that are utilized in computing the token outputs. The authentication entity performing the verification of the token outputs requires access to one or more seeds associated with the token in question. Typically, such authentication entities have access to the same seed or set of seeds that the token uses to generate its output.

Please replace the paragraph beginning on page 5, line 1, with the following replacement paragraph:

In an illustrative embodiment, the processing device 102S comprises or is otherwise associated with an authentication entity, such as a server or other processing device equipped with ACE/~~Server~~SERVER® software, and the processing device 102C comprises or is otherwise associated with an authentication token, such as an RSA ~~SecurID~~SECURID® authentication token. Although this embodiment is presented in the context of an authentication token, the described techniques are adaptable in a straightforward manner to a wide variety of other cryptographic processing devices.

Please replace the paragraph beginning on page 15, line 25, with the following replacement paragraph:

The SSGP server decrypts R_C and generates a seed by applying a hash function to a combination of R_S, K_S and R_C. The SSGP client also generates a seed in a similar manner, although this operation is not explicitly shown in the figure. The SSGP server registers the user and generated seed with an authentication entity, such as a server equipped with RSA ACE/~~Server~~SERVER® software. The SSGP server then sends a commit message to the SSGP client. The SSGP client then stores the serial number with the generated seed.